

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-199508

(P2004-199508A)

(43) 公開日 平成16年7月15日(2004.7.15)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
G06F 15/00	G06F 15/00 330G	5B085
G06F 17/60	G06F 17/60 140	5J104
H04L 9/32	G06F 17/60 506	5K024
H04M 3/42	G06F 17/60 512	5K101
H04M 11/00	H04M 3/42 C	

審査請求 有 請求項の数 7 O L (全 8 頁) 最終頁に続く

(21) 出願番号	特願2002-368877 (P2002-368877)	(71) 出願人	502458431 株式会社アイシーシーエー
(22) 出願日	平成14年12月19日 (2002.12.19)		東京都渋谷区代々木4-31-4-1201
		(74) 代理人	100105371 弁理士 加古 進
		(72) 発明者	河野 真太郎 神奈川県横浜市青葉区荏子田2-25-2-A
		(72) 発明者	加来 徹也 東京都千代田区神田小川町3-1 株式会社コネクト内
		(72) 発明者	長岡 大輔 東京都千代田区神田小川町3-1 株式会社コネクト内

最終頁に続く

(54) 【発明の名称】 認証システム

(57) 【要約】

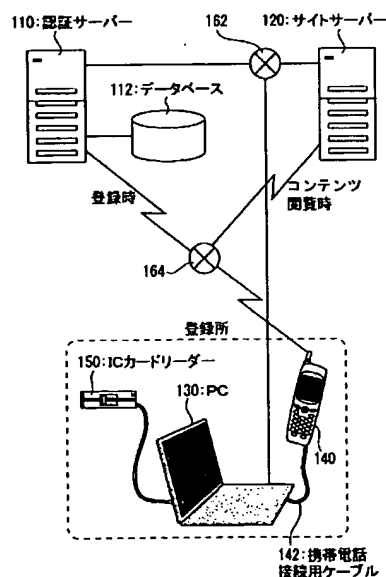
【課題】 携帯電話等を使用して、確実に本人確認に用いられる認証システムを提供する。

【解決手段】 認証を受けるための登録は「登録所」で行っている。登録したい人（登録人）は、登録所の登録作業を行う人（登録者）に、本人確認のために公式な書類（免許証、パスポート等）を提示する。

登録者は、登録者自身に与えられたICカードで、登録者の認証を行った上で、登録人の携帯電話140をパソコン130とケーブル142で接続し、認証サーバー110に対する登録作業を行う。携帯電話140のデータは、認証サーバー110のデータベース112に格納される。

登録人が成人対象のビジネスに参加するため、そのビジネスを運用するサイトサーバー120に携帯電話140によりアクセスしたとき、認証サーバー110に対して成人であるかの確認を携帯電話140が登録されているかにより行う。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

携帯電話を電気通信回線を介して登録して認証を行う認証システムであって、登録端末システムと認証サーバーシステムを有しており、
前記登録端末システムは、
前記認証サーバーシステムと、電気通信回線を介して接続する接続手段と、
乱数を発生する乱数発生手段と、
前記乱数発生手段で発生した乱数を前記認証サーバーシステムに送る乱数送信手段と、
前記携帯電話とを接続する携帯電話接続手段と、
前記携帯電話から、前記携帯電話接続手段を介して、前記乱数発生手段で発生した乱数と
、前記携帯電話の固有 ID とを前記認証サーバーシステムに送る手段とを備え、前記認証
サーバーシステムは、
前記登録端末システムから送られた乱数を受信する第 1 の受信手段と、
前記携帯電話からの乱数及び固有 ID を受信する第 2 受信手段と、
前記第 1 の受信手段からの乱数と、前記第 2 受信手段からの乱数との一致を調べる一致検
出手段と、
前記一致検出手段で、一致が検出されたとき、前記第 2 受信手段で受信した前記携帯電話
の固有 ID を登録する登録手段と
を備えることを特徴とする認証システム。

20

【請求項 2】

携帯電話を、電気通信回線を介して認証サーバーシステムに登録するための登録端末システムであって、
前記認証サーバーシステムと、電気通信回線を介して接続する接続手段と、
乱数を発生する乱数発生手段と、
前記乱数発生手段で発生した乱数を前記認証サーバーシステムに送る乱数送信手段と、
前記携帯電話とを接続する携帯電話接続手段と、
前記携帯電話から、前記携帯電話接続手段を介して、前記乱数発生手段で発生した乱数と
、前記携帯電話の固有 ID とを前記認証サーバーシステムに送る手段と
を備えることを特徴とする登録端末システム。

30

【請求項 3】

登録端末システム及び携帯電話と電気通信回線を介して接続している認証サーバーシステムであって、
前記登録端末システムから送られた乱数を受信する第 1 の受信手段と、
前記携帯電話からの乱数及び固有 ID を受信する第 2 受信手段と、
前記第 1 の受信手段からの乱数と、前記第 2 受信手段からの乱数との一致を調べる一致検
出手段と、
前記一致検出手段で、一致が検出されたとき、前記第 2 受信手段で受信した前記携帯電話
の固有 ID を登録する登録手段と
を備えることを特徴とする認証サーバーシステム。

40

【請求項 4】

請求項 1 に記載の認証システムにおいて、
前記登録端末システムの前記乱数送信手段は、前記乱数を秘密カギで暗号化して送信し、
前記認証サーバーシステムの前記第 1 の受信手段は、前記乱数を公開カギで復号して、
前記登録端末システムの認証を行うことを特徴とする認証システム。

【請求項 5】

請求項 3 に記載の認証サーバーシステムにおいて、
サービスを行うサイトサーバーシステムから送られた前記携帯電話の固有 ID を、電気通
信回線を介して受信する固有 ID 受信手段と、
前記固有 ID が前記登録手段に登録されているかを調べる認証手段と、
前記認証手段の結果を、前記サイトサーバーシステムに認証結果として、電気通信回線を

50

介して送信する送信手段と

を備え、携帯電話の固有IDにより認証することを特徴とする認証サーバシステム。

【請求項6】

請求項5に記載の認証サーバシステムにおいて、

前記サイトサーバシステムから求める認証は、成人であることの認証であることを特徴とする認証サーバシステム。

【請求項7】

請求項2に記載の登録端末システムをコンピュータシステムに構築するプログラム。

【発明の詳細な説明】

【0001】

10

【発明の属する技術分野】

本発明は、本人確認に用いられる携帯電話等を使用した認証システムに関し、特に成人であることを確認することができる認証システムに関する。

【技術的背景】

成人であることを確認するには、クレジットカード番号を使った与信システムにて行う方法があるが、親の承認により未成年（18歳未満）でもクレジットカードが持てる時代で不正に登録されてしまうことが可能になり、成人認証の確実な方法とはならなくなった。成人（18歳以上）を対象にした携帯電話ビジネスで、そのビジネスを運用している側では、その携帯電話の使用者が成人（18歳以上）であるかを確認する良い手段が無く、気軽に未成年者（18歳未満）に参加される場合が増えてきている。この場合、色々な問題

20

が起きており、社会問題となっている。

【0002】

【発明が解決しようとする課題】

本発明の目的は、携帯電話等を使用して、確実に本人確認に用いられる認証システムに関し、特に成人であることを確認することができる認証システムを提供しようとするものである。

【課題を解決するための手段】

本発明の目的を達成するために、本発明は、携帯電話を電気通信回線を介して登録して認証を行う認証システムであって、登録端末システムと認証サーバシステムを有しており、前記登録端末システムは、前記認証サーバシステムと、電気通信回線を介して接続する接続手段と、乱数を発生する乱数発生手段と、前記乱数発生手段で発生した乱数を前記認証サーバシステムに送る乱数送信手段と、前記携帯電話とを接続する携帯電話接続手段と、前記携帯電話から、前記携帯電話接続手段を介して、前記乱数発生手段で発生した乱数と、前記携帯電話の固有IDとを前記認証サーバシステムに送る手段とを備え、前記認証サーバシステムは、前記登録端末システムから送られた乱数を受信する第1の受信手段と、前記携帯電話からの乱数及び固有IDを受信する第2受信手段と、前記第1の受信手段からの乱数と、前記第2受信手段からの乱数との一致を調べる一致検出手段と、前記一致検出手段で、一致が検出されたとき、前記第2受信手段で受信した前記携帯電話の固有IDを登録する登録手段とを備えることを特徴とする。

30

【0003】

40

携帯電話を電気通信回線を介して認証サーバシステムに登録するための登録端末システムは、前記認証サーバシステムと、電気通信回線を介して接続する接続手段と、乱数を発生する乱数発生手段と、前記乱数発生手段で発生した乱数を前記認証サーバシステムに送る乱数送信手段と、前記携帯電話とを接続する携帯電話接続手段と、前記携帯電話から、前記携帯電話接続手段を介して、前記乱数発生手段で発生した乱数と、前記携帯電話の固有IDとを前記認証サーバシステムに送る手段とを備えることを特徴とする。

登録端末システム及び携帯電話と電気通信回線を介して接続している認証サーバシステムであって、前記登録端末システムから送られた乱数を受信する第1の受信手段と、前記携帯電話からの乱数及び固有IDを受信する第2受信手段と、前記第1の受信手段からの乱数と、前記第2受信手段からの乱数との一致を調べる一致検出手段と、前記一致検出手

50

段で、一致が検出されたとき、前記第2受信手段で受信した前記携帯電話の固有IDを登録する登録手段とを備えることを特徴とする。

【0004】

また、認証システムでは、前記登録端末システムの前記乱数送信手段は、前記乱数を秘密カギで暗号化して送信し、前記認証サーバーシステムの前記第1の受信手段は、前記乱数を公開カギで復号して、前記登録端末システムの認証を行うこともできる。

認証サーバーシステムにおいては、サービスを行うサイトサーバーシステムから送られた前記携帯電話の固有IDを、電気通信回線を介して受信する固有ID受信手段と、前記固有IDが前記登録手段に登録されているかを調べる認証手段と、前記認証手段の結果を、前記サイトサーバーシステムに認証結果として、電気通信回線を介して送信する送信手段とを備え、携帯電話の固有IDにより認証することもできる。

認証サーバーシステムにおいて、サイトサーバーシステムから求める認証は、成人であることの認証であることもできる。

登録端末システムをコンピュータシステムに構築するプログラムも本発明である。

【0005】

【発明の実施の形態】

本発明の実施の形態を、図面を参照して説明する。

図1は、本発明のシステム構成例を示す。図1に示すように、認証を受けるための登録は「登録所」で行っている。登録したい人（登録人）は、登録所の登録作業を行う人（登録者）に、本人確認のために公式な書類（免許証、パスポート等）を提示する。

登録所は、インターネット162を介して認証サーバー110と接続しているパソコン（PC）130と、パソコン130と接続しているICカードリーダー150とで構成している。パソコン130には、携帯電話を認証サーバーに登録するために、登録用のプログラムがインストールされている。登録者は、登録者自身に与えられたICカードをカードリーダー150に読み取らせることにより、登録者の認証を行った上で、登録人の携帯電話140をパソコン130とケーブル142で接続し、認証サーバー110に対する登録作業を行う。登録された登録人の携帯電話140のデータは、認証サーバー110のデータベース112に格納される。

登録人が成人（18歳以上）対象のサービスに参加するため、そのビジネスを運用するサイトサーバー120に携帯電話140を用いてアクセスする。このとき、認証サーバー110に対して成人であるかの確認を、認証サーバー110に携帯電話140が登録されているかにより行う。もし、登録されていない携帯電話からのアクセスなら、登録所にて登録することを促し、登録した携帯電話のアクセスならサービスへの参加を認める。

これらの成人向け携帯電話ビジネスをする者は、このシステムもしくはこれ同等のシステムを使わず未成年者を参加させた場合には、法的な処理を受けるようにすることも考えられる。

【0006】

まず、登録処理について、図2の機能ブロック図及び図3のシーケンス図を用いて詳しく説明する。

図2は、携帯電話を登録・認証する認証サーバー110、携帯電話を用いたサービスを提供するサイトサーバー120、及び登録を行う端末であるパソコン（PC）130が備えている機能を示す機能ブロック図である。

認証サーバー110は、登録処理のために、公開カギによる登録者認証と、データベース112に対する登録の機能114を有している。また、サービスを行っているサイトからの認証を行うときに必要なサイト認証のために、共通カギによるサイト認証の機能116も有している。

また、登録所に設置されているパソコン130には、乱数発生131、登録人のデータ（例えば、年齢や免許no等）を入力133、サーバーとの通信135、携帯電話とのケーブル接続を介して、携帯電話のキーボードからの入力と同じ様に入力を行うことができるキーボードエミュレーション132、PKI（公開鍵基盤）を用いた暗号化137、ケー

ブル接続された携帯電話の機種を判別する機種判別 136 等の機能を有している。
サービスを提供するサイトサーバー 120 には、サービスを提供するための例えば WEB
機能 126 等と、認証サーバー 110 との間で、認証を行うための、共通カギや ID 等を
格納しておくためのキャッシュ DB 等の機能を実装した認証モジュール 122 を有してい
る。

上述の各機能や機能を実現するための手法は従来から知られているおり、ここでは各機能
について詳しく説明しない。

【0007】

さて、登録所を訪れた登録人は、公的な書類（運転免許証等）で本人であることを登録所
の登録者に証明する。登録所の登録者は、登録人を認証サーバー 110 に登録する処理を 10
行うために、まず、ICカード 152 をパソコン 130 に読み取らせる（S202）。IC
カード 152 には、登録者に対応した秘密カギが格納してあり、パソコン 130 は、IC
カード 152 から秘密カギを読み取り、この秘密カギを認証サーバー 110 に対して登
録処理を行う登録者の認証に用いる。

登録者は、次に、携帯電話 140 をシリアルケーブル 142 で PC 130 と接続して、携
帯電話の登録処理を開始する。PC 130 は乱数を生成し（S204）、ICカード 15
2 から読み取った秘密カギで暗号化して PC 130 からサーバー 110 に送信する（S2
06）。PC 130 は、同時にシリアルケーブル 142 を介して、携帯電話 140 にサー
バー 110 へ接続するためのキーボード・エミュレーションを要求する（S208）。P
C 130 は、携帯電話 140 の機種を判別して、判別した機種にあった処理を行う。携帯 20
電話 140 は、PC 130 からのキーボード・エミュレーションで認証サーバー 110 に
接続し、接続パラメータとして OneTimeID と MachineID（機械 ID）を送出する（S210
）。MachineID は、携帯電話の製造番号であり、携帯電話ごとに異なる番号で、ウェブサ
ーバー側から読み出すことができる。ここでは、MachineID を用いているが、認証に用い
る ID は携帯電話固有の ID で外部から読み出せるものであればよい。

サーバー 110 では、公開カギを使って PC 130 から送られた暗号化を解き（S214
）、解けたことで登録者本人の認証とされる。サーバー 110 で暗号化を解いて出てきた
PC 130 からの乱数と、携帯電話 140 からの OneTimeID（乱数）を比べ（S216）、
一致したときにデータベースへの登録をする（S218）とともに、PC 130 へ登録完
了通知を行う（S220）。一致しない場合は、エラー表示を行う。登録通知として、サ
ーバー 110 から携帯電話 140 に OK と表示（S222）されれば、登録処理は完了す
る。PC 130 からも暗号化して送られる OneTimeID を用いているので、PC 130 と接
続している携帯電話 140 のみを、真正な登録される携帯電話として登録することができ
る。

【0008】

サイトサーバー 120 による個人認証の処理について、図 2 の機能ブロック図、図 4 のシ
ーケンス図、及び図 5 の携帯電話の画面の図を用いて説明する。

サイト 120 には、サーバー内に認証サーバー 110 にアクセスして個人認証を行うため
の認証モジュール 122 を入れておく。この認証モジュール 122 は、サーバー 120 に
対して携帯電話 140 からアクセスがあったとき、認証サーバー 110 との認証処理を行
う。認証モジュール 122 にはモジュールの発行時に、共通カギとして使用する Domain N
ame（サーバー 120 の IP アドレス）が埋め込まれているので、不定使用を防ぐことがで
きる。 40

例えば、成人用のサービスを行っているサーバー 120 に対して携帯電話 140 からアク
セスがあったとき（図 4：S302）に、サーバー 120 は、18 歳以上かをたずねる画
面を出して（図 5：410）、18 歳以上であることが選択されると、認証モジュール 1
22 にジャンプして（図 5：420）、アクセスした携帯電話 140 の MachineID を要求
する（S304）。携帯電話 140 から MachineID を得る（図 4：S306、図 5：43
0）と、この MachineID が、すでに認証モジュール 122 内のキャッシュ DB 124 にあ
る場合は、認証済みななので、すぐにサーバーのサービスを開始する（図 4：S320、図 50

5:440)。

携帯電話から得たMachineIDがキャッシュにない場合、共通カギでMachineIDを暗号化して認証サーバーに送る(図4:S308)。認証サーバーでは、共通カギで暗号化したMachineIDを復号して、登録されているMachineIDかどうかで認証を行い、認証サーバー110からOKが返ってきた(図4:S312, 図5:440)ときのみ、サイトに入れるようにする。携帯電話が登録されていない場合は、登録所において登録するように勧める(図5:460)。

この認証システムは、携帯電話を使った出会い系サイトビジネス、携帯電話を使った自動販売機での未成年者確認、未成年者犯罪防止、携帯電話による本人確認システム等に適用することができる。

10

【0009】

【発明の効果】

このシステムを使うことで、不正なく携帯電話の登録ができ、例えば未成年者のアクセスを排除できる。また、このシステムの導入により、故意に未成年者の参加を許可している業者や、不正な方法で入手した携帯電話を特定してその使用者に対して法的な処置も可能になる。

【図面の簡単な説明】

【図1】実施形態のシステム構成図である。

【図2】実施形態の機能ブロック図である。

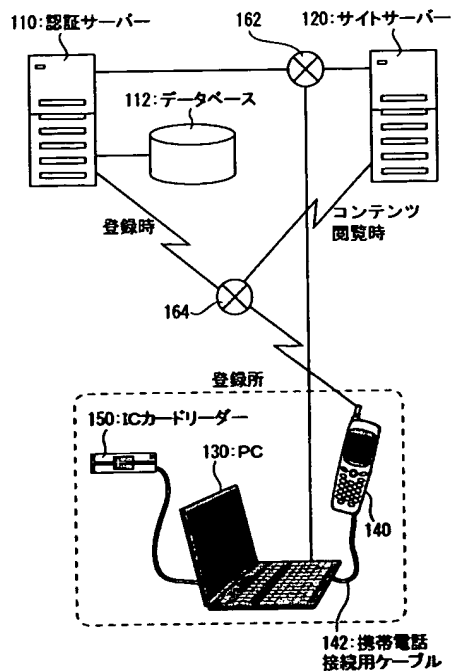
【図3】登録処理のシーケンス図である。

【図4】認証処理のシーケンス図である。

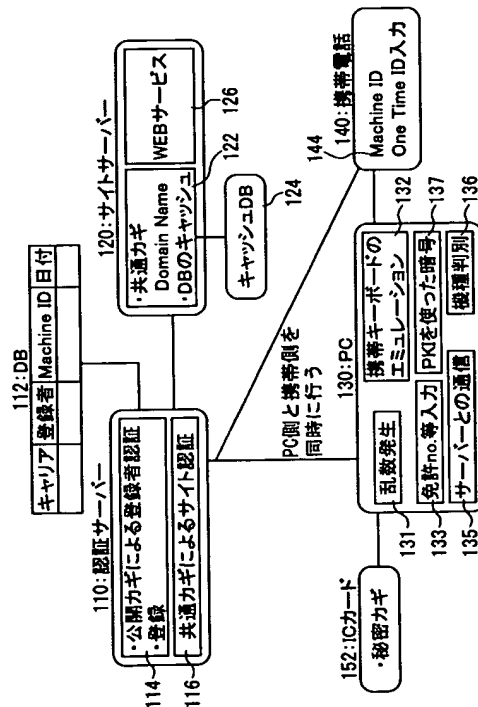
【図5】認証処理における携帯電話の画面の例を示す図である。

20

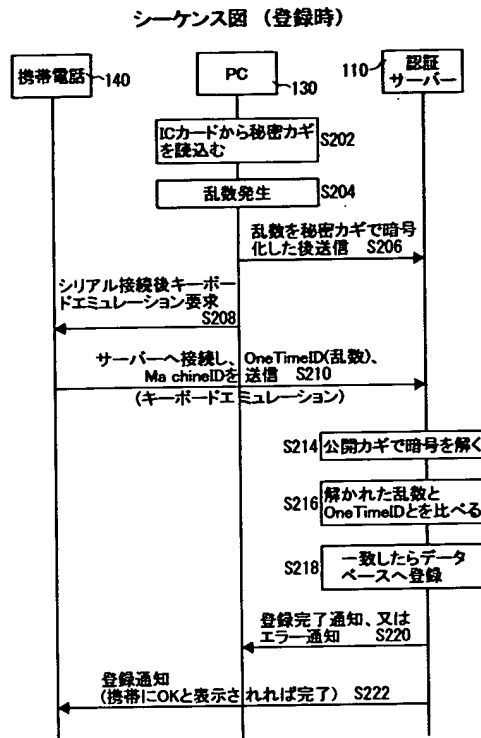
【図1】



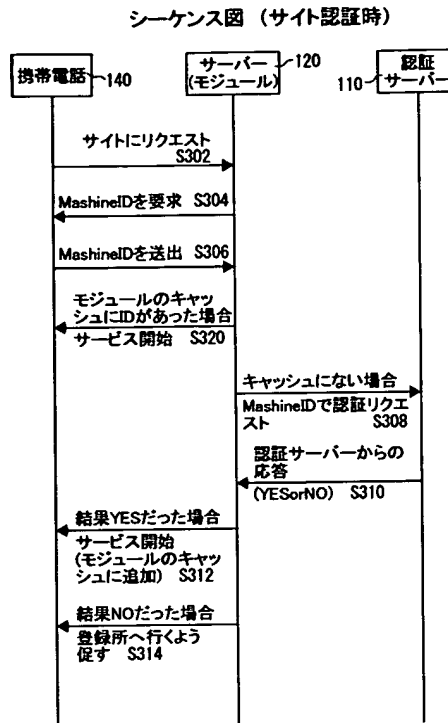
【図2】



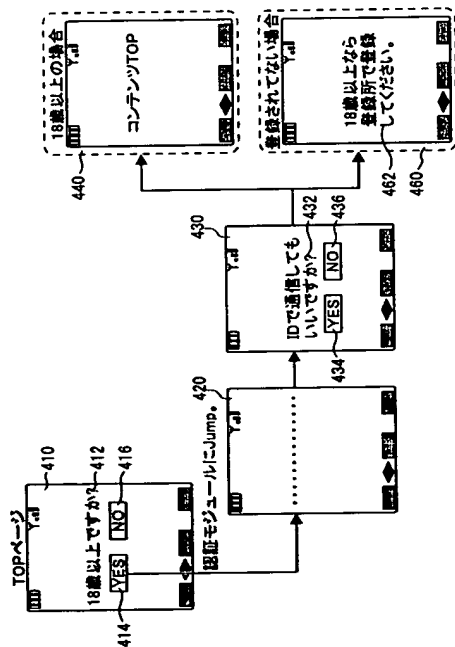
【図 3】



【図 4】



【図 5】



フロントページの続き

(51)Int. Cl.⁷

F I

テーマコード (参考)

H 0 4 M	11/00	3 0 2
H 0 4 L	9/00	6 7 3 B
H 0 4 L	9/00	6 7 5 D

(72)発明者 新海 昇

東京都新宿区高田馬場3-3-3 アールピーエー株式会社内

Fターム(参考) 5B085 AE01 AE08 AE11

5J104 AA07 KA01 PA01 PA10

5K024 AA72 AA74 AA76 BB04 CC11 DD01 DD02 EE08 FF03 GG05

GG06 GG08

5K101 KK15 KK16 LL12 MM07 NN05 NN18 NN21 PP03 PP04